PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification [7] : H04N 1/32	**A1**	**(11) International Publication Number:** **WO 00/18109**
		(43) International Publication Date: 30 March 2000 (30.03.00)

(21) International Application Number: PCT/EP99/07024

(22) International Filing Date: 21 September 1999 (21.09.99)

(30) Priority Data:
09/159,288   23 September 1998 (23.09.98)   US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL–5621 BA Eindhoven (NL).

(72) Inventors: LORD, William, P.; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL). ABDEL–MOTTALEB, Mohamed; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL). EPSTEIN, Michael, A.; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(74) Agent: HOEKSTRA, Jelle; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(81) Designated States: CN, JP, KR, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD FOR CONFIRMING THE INTEGRITY OF AN IMAGE TRANSMITTED WITH A LOSS

(57) Abstract

A digital image is divided into a plurality of cells having a first sequence. A random seed is generated and used to produce two sets of pseudo–random numbers. The first set of pseudo–random numbers are used to alter the location and shape of the cells thereby creating a new set of cells that the image is divided into. A measurement is taken for each of these new cells. The second set of pseudo–random numbers creates a second sequence. Each of the new cells corresponding to the first sequence is compared to another new cell corresponding to the second sequence. This comparison is related to a threshold and yields a fingerprint. The resultant fingerprint is transmitted along with the image and the random seed. A receiver performs the same algorithm on its received image. If it produces the same fingerprint as the one it receives, it is assumed that the image has not been altered.

Method for confirming the integrity of an image transmitted with a loss.

5

The present invention relates generally to the field of signal encryption and more specifically, to a method for identifying whether digital images, transmitted with a loss, have been unaltered and have been sent from a specific source. This is accomplished through the creation of a specialized fingerprint and "signature".

10

Methods exist for encrypting digital signals to prevent tampering such as disclosed in United States Patent No. 5,499,294, keep a malicious adversary from altering the signal. A fingerprint or "hash" is taken of the digital image. Hashing algorithms (i.e. one-way functions) are well known and easy to calculate but very difficult to mathematically invert.

15   The fingerprint is typically encrypted with an encryption key to prove or authenticate the creator of the signature. The encryption itself is a standard public/private key cryptology with the source station utilizing a private key. The resulting signature can be decrypted by a receiving station with the source's public key.

20   The hash-key combination along with the original image, is then sent to the receiving station which uses the public key of the presumed transmitter in decrypting the encrypted hash. The receiving station performs the same hash algorithm on the received image and compares it to the decrypted hash. If these two hashes are identical, there has been no noise in the transmission and the image has not been modified (tampered) by a third party. If

25   the image was modified or the wrong public key is used, the two hashes will not be identical.

The same technique would generally not work in a transmission where information is lost. Generally, a digitized version of a received image includes lost bits or noise which corrupt the received digitized image. Consequently, it is difficult to confirm whether a received image has been tampered with based upon a comparison of the received

30   fingerprint of the source image to a digitized fingerprint generated based on the received digitized image.

Another attempt to solve the problem in a JPEG transmission is described in "A Robust Image Authentication Algorithm Distinguishing JPEG Compression from Malicious Manipulations" by Ching-Yun Lin and Shih-Fu Chang, published in ISLT/SPIE Symposium

on Electronic Imaging: Science and Technology. Jan 1998, San Jose, Cal. pages 77-80. Their method is to compare the same block in subsequent frames of a JPEG compressed transmission. This comparison is performed to ensure that the range of difference in value between these two blocks remains the same even after compression and decompression is

5   performed. A signature is created by comparing the difference between two blocks and a threshold. A binary "0" or "1" is entered into the signature depending on whether the difference is above or below that threshold. This signature is sent along with the transmitted image and the method continues as discussed above.

The Lin/Chang method is deficient in that it relies on the inherent structure of

10 JPEG compression and would not work with other transmissions (including lossy transmissions) which do not follow the JPEG format. Further, The Lin/Chang method allows the possibility of tampering. Since the signature is completely based upon a comparison of consecutive frames with a threshold, a malicious adversary could create a completely different data stream and send it to the receiver as long as the differences between consecutive frames is

15 approximately (within the range of the chosen threshold) the same.

Still another technique known in the art is watermarking. A set of bits (a mark) is added to a transmitted image. This mark should be complete enough so that it can be detected by a receiver but should not alter the nature of the image. The technique is often used in copyright situations where piracy is a concern. A defendant who alleges he did not copy the

20 image will then be forced to explain why the watermark is still within the image. Watermarking is an efficient way of proving origination. However, it does not indicate when tampering has occurred.

Therefore, it is desirable to provide an improved method for confirming whether a received image has been altered. The method should include a fingerprint which is

25 simple to compute from the image but difficult to create an image that has a given fingerprint. The fingerprint method also should have the characteristic that it would be difficult to generate two images that have the same fingerprint. The fingerprint method should be operable when losses are experienced through transmission of the digitized signal.

One aspect of the invention is a method for confirming the integrity of a

30 transmitted image including the steps of dividing the image into a first plurality of cells having a first sequence, generating a random seed and generating a first plurality of pseudo random numbers based upon said random seed. The method further includes the steps of creating the image into a second plurality of cells based upon the first plurality of pseudo random numbers and the first plurality of cells and generating a second plurality of pseudo random numbers, the

second plurality of pseudo random numbers forming a second sequence. The method also includes the steps of comparing cells corresponding to the first sequence with cells corresponding to the second sequence, in forming a first fingerprint, and transmitting the fingerprint, the image, and the random seed to a receiver. The method still further includes the steps of producing a second fingerprint, by the receiver, using the image and the random seed that was received, and comparing the first and second fingerprints.

This method makes it difficult for a third party to manipulate an image without changing the fingerprint of that image. The fingerprint itself is easy to create if one knows the seed. But, this seed will be unknown by a third party. Even though the image will be sent with losses, the fingerprint will not change and so it still can be used to monitor the integrity of the image.

Another aspect of the present invention is a method for creating a fingerprint of an image including the steps of dividing the image into a first plurality of cells having a first sequence, generating a random seed, generating a first plurality of pseudo random numbers based upon the random seed, and dividing the image into a second plurality of cells based upon the first plurality of pseudo random numbers and the first plurality of cells. The method also includes the steps of generating a second plurality of pseudo random numbers, the second plurality of pseudo random numbers forming a second sequence, and comparing cells corresponding to the first sequence with cells corresponding to the second sequence, in forming the fingerprint. This fingerprint has the same benefits as the fingerprint stated above.

In yet another aspect of the invention a computer readable storage medium includes a fingerprint representing an image, the medium has a series of representations, each representation resulting from a comparison between a threshold and a difference between a first number and a second number. The first number corresponds to a value of a first cell of a first plurality of cells of the image. The second number corresponds to a value of a second cell of a second plurality of cells of the image. The first plurality of cells is formed by dividing the image into a third plurality of cells and manipulating the third plurality of cells based upon a first plurality of pseudo random numbers. The second plurality of cells are equal in number to said first plurality of cells and have a sequence dictated by said second plurality of pseudo random numbers.

In still yet another aspect of the present invention, a computer readable storage medium has encoded data for dividing an image into a first plurality of cells having a first sequence, generating a random seed, and generating a first plurality of pseudo random numbers based upon the random seed. The medium further has data for creating the image into

a second plurality of cells based upon the first plurality of pseudo random numbers and the first plurality of cells, generating a second plurality of pseudo random numbers, the second plurality of pseudo random numbers forming a second sequence, and comparing cells corresponding to the first sequence with cells corresponding to the second sequence, in forming a fingerprint.

It is an object of the invention to provide a method for verifying the source and integrity of an image transmitted with a loss.

It is another object of the present invention to provide a signature of a digital image that is unique, easily produced, and capable of comparison with another signature even after being transmitted with loss.

These and other objects will become apparent from the following disclosure with continuing reference to the drawings where like reference numerals refer to the same element.

Fig. 1 is a diagram showing the division and ordering of cells of an image to be transmitted according to the invention;

Fig. 2 is a diagram showing newly created cells in accordance with the invention;

Fig. 3 is a diagram of a representative fingerprint in accordance with the invention;

Fig. 4 is a flow chart of a method for generation of a signal to be transmitted representing, in part, the image and fingerprint of Fig. 3; and

Fig. 5 is a flow chart of a method for receiving a transmitted image and fingerprint of Fig. 3 and for confirming the integrity of that image.

Referring to Figs. 1 and 4, a n x n grid 100 is applied to a source digital image 103 thereby creating n^2 cells under step 200. The value of n depends upon the processing power and probability of accuracy desired. The n^2 cells are numbered (C1, C2, C3. . .Cn^2) in accordance with any suitable numbering system desired. Under step 202, a random seed "r" is generated. The best way to make this random seed is from a source in nature. For example,

5

electrical noise, radioactive decay, or cosmic rays from the sun. Anything unpredictable that can not be altered easily would form an optimal source. At step 204, using r as a seed, n^2 pseudo-random numbers (prn) are generated. A boundary must be imposed on the prn values because of the displacement caused by these numbers (as will be explained in more detail

5 below) These numbers are calculated using a mathematical algorithm applied to random number r. Any algorithm could be used. Although the algorithm may eventually be determined, random seed r can not be easily learned.

Referring now to Fig. 2, under step 206 each cell (C1, C2, C3. . .Cn^2) is then manipulated (i.e. displaced and scaled) as a result of its respective prn. For example, each cell

10 could be displaced from its origin by the prn and then the width and height changed by the same amount (or by a different amounts generated by multiple prns) as the displacement. If displacement causes a cell to go beyond the original image's boundaries, the cell wraps around to the other side as shown in Fig. 2. As is evident, many cells now overlap. The size and location of these new cells (C1', C2', C3'. . .$Cn^{2'}$) is unknown to a third party.

15 Prior art fingerprints produced an evaluation metric for each cell thereby creating a corresponding value. Many techniques could be used to find this metric. For example, the measure could be the amount of a particular color in each cell, a sum of the values of the pixels, or a discrete cosine transform ("DCT"). In these prior art fingerprints, as was stated above, a third party could easily create a different image that would have the same

20 fingerprint. If green were the variable, for example, a third party would merely have to produce cells which have the same amount of green in them. However, if a third party attempted to recreate an image with the fingerprint of the present invention, he would interfere with multiple overlapping cells.

At step 208, for each of these newly created cells, an evaluation metric is taken

25 for each resulting area of the image. The actual measure used is not important and any of the prior art techniques could be implemented. Experimentation has found that if a DCT is used only the DC value is necessary; the AC values do not significantly contribute to the calculation. An assortment of techniques could be available and chosen by a user or randomly chosen using the pseudo-random numbers described above. This assortment of techniques

30 could also be combined together to form one large signature. The goal is to make a signature so that it would be difficult for a third party to create a different image with the same signature.

Under step 210, a second set of n^2 pseudo-random numbers is created. These numbers represent a sequence to be applied to the newly generated cells. The first number in

the sequence is the cell number that is compared with cell 1, the second number is the cell number compared with cell 2, and the n^2 number is the cell number compared with cell n^2. For example, if the second set of prns started with 14, 23, 5. . ., then cell 14 would be compared with cell 1, cell 23 with cell 2 and so on. The comparison is the relation of the metric values that were determined above.

At step 212, a fingerprint is created by comparing the relationship between the pairs to a threshold. If the difference between a pair is above the threshold, a "1" is entered into the fingerprint. Otherwise, a "0" is entered. Each pair thus produces one bit of a fingerprint that is n^2 bits long. An example of a fingerprint is shown in Fig. 3. The fingerprint could be stored on any storage medium or can be transmitted immediately.

For transmission from a transmitter A to a receiver B, random seed r is encrypted with the public key of the receiver - $E_{pub(b)}(r)$ under step 214. The fingerprint is then appended to $E_{pub(b)}(r)$. Finally, the $E_{pub(b)}(r)$ and fingerprint combination are encrypted with the private key of the sender and sent - $E_{pri(a)}[E_{pub(b)}(r)$ and fingerprint] under steps 216 and 218. Clearly, the $E_{pub(b)}(r)$ does not have to be encrypted with the A private key. But, if not, at least the fingerprint would require the private key of A so that origination at A could be verified.

Both the fingerprint and the image are sent. The image is sent in the same way as it would have been. As for the fingerprint, even analog transmissions still allot for digital data that can be sent with some loss. For example, if an NTSC standard is used, digital data may be sent during the vertical blanking interval (VBI). In NTSC, pixels are illuminated horizontally, row by row. When the last pixel is energized, a finite period of time is required to traverse back to the beginning of the screen. During this time, called the VBI, digital data can be received. Other similar periods exist in equivalent standards.

Referring to Fig. 5, on the receiving side B, the image and fingerprint are decrypted using A's public key. The result will be nonsensical if any other source but A sent the message. If the wrong public key is used (for example a third station C), the result will also not make sense. The receiver now has the signature and E(r) and uses its own private key to obtain r. Receiver B performs the same steps on the image it received as A performed previously. Those steps include: dividing the image into an n-by-n grid, generating pseudo-numbers, etc. This will also produce a fingerprint of the image received. The receiving station compares this generated fingerprint with the fingerprint received. These two fingerprints should be the same. The comparison could be in real time or the fingerprints could be stored

and compared later. Even though there is loss in the transmission, that loss should not affect the fingerprint so much that it will significantly change.

Some difference in the signatures could be allowed in order to compensate for noise in the transmission. For example the two fingerprints could be compared and the differences between them (the number of 0s and 1s that do not match) could be acceptable if below a threshold ("Hamming" distance). Even allotting for some bits in the fingerprints being different would not affect the security of the system because tampering would cause many bits in a fingerprint to flip; noise should only cause a few changes.

Clearly, all of the above variables can be modified without affecting the inherent nature of the algorithm. For example, the number of cells created, n, could be increased or decreased depending upon the security desired by a user.

The foregoing discloses an enhanced way for confirming the integrity and authenticity of a transmitted signal. The invention produces at least four cognizable results which optimize the operation of the system: 1) the size of each cell used is unknown by a third party. This is protected by the prns which are produced by an unknown random seed. The actual sizing and scaling algorithm could be also be secret. 2) A third party does not know which cells are compared. This is also a function of an unknown random variable. 3) The location of the cells is unknown as they are also a function of the generated random variable. 4) The algorithm or evaluation metric used to evaluate each cell is unknown. As stated above, the metric used could be a function of the prns as well.

For an additional element of security, a time stamp could be added to the transmitted signal. A malicious third party may be able to access the image and then send a delayed image to the receiver thereby transmitting an acceptable image and fingerprint. A time stamp would avoid this problem because the time would now also be included in the transmission. This stamp would be encrypted and sent to the receiver along with r, the computed fingerprint, and the image.

Clearly the exact order of the steps shown above need not be followed. For example, all the pseudo-random numbers could be created at the same time even before the n by n grid is applied.

As can now be readily appreciated, the invention, through the creation of a specialized fingerprint, thereby allows a evaluation to be made as to whether a transmitted image is unaltered, even when there was loss in the transmission.

Having described the preferred embodiments it should be made apparent to those skilled in the art that various changes may be made without departing from the scope or spirit of the invention as is defined more clearly in the appended claims.

CLAIMS:

1.   A method for creating a fingerprint of an image comprising the steps of:

dividing said image into a first plurality of cells having a first sequence (200);

generating a random seed (202);

generating a first plurality of pseudo random numbers (204) based upon said

5   random seed;

dividing said image into a second plurality of cells based upon said first

plurality of pseudo random numbers and said first plurality of cells (206);

generating a second plurality of pseudo random numbers (210), said second

plurality of pseudo random numbers determining a second sequence of said second plurality of

10   cells; and

comparing cells corresponding to said first sequence with cells corresponding to

said second sequence, in forming said fingerprint (212).

2.   The method of claim 1 wherein said step of dividing comprises moving and

15   scaling said first plurality of cells.

3.   The method of claim 1 wherein said first plurality of cells is equal in number to

said first plurality of pseudo random numbers and equal in number to said second plurality of

pseudo random numbers.

20

4.   The method of claim 1 wherein said step of comparing the cells includes

evaluating each cell using a plurality of evaluation metrics.

5.   The method of claim 1 wherein said step of comparing the cells includes

25   evaluating each cell using an evaluation metric chosen from a plurality of evaluation metrics,

said choice being dictated by at least one of said first and second plurality of pseudo random

numbers.

6.   A method for confirming the integrity of a transmitted digital image
comprising the following steps:

          creating a fingerprint of an image according to the method as claimed in claim
1;

          transmitting said fingerprint, said image, and said random seed to a receiver
(218);

          producing a second fingerprint, by said receiver, using said image and said
random seed that was received (316); and

          comparing said first and second fingerprints (318).

7.   The method of claim 6 wherein said step of transmitting comprises the steps of:
          encrypting said random seed with a public key of said receiver (214) thereby
producing an encrypted seed; and
          encrypting said first fingerprint and said encrypted seed with a private key of
said transmitter (216).

8.   The method of claim 6 further comprising the steps of:
          generating a time stamp; and
          transmitting said time stamp to said receiver.

9.   The method of claim 6 wherein said second fingerprint is formed in the same
way as said first fingerprint.

10.   A security system using the method of claim 1 or 6.

11.   A computer readable storage medium including a fingerprint representing an
image, said fingerprint comprising:

          a series of representations, each said representation resulting from a comparison
between a threshold and a difference between a first number and a second number;

          said first number corresponding to a value of a first cell of a first plurality of
cells of said image;

          said second number corresponding to a value of a second cell of a second
plurality of cells of said image;

said first plurality of cells being formed by dividing said image into a third plurality of cells and manipulating (206) said third plurality of cells based upon a first plurality of pseudo random numbers (204); and

said second plurality of cells being equal in number to said first plurality of cells and having a sequence dictated by said second plurality of pseudo random numbers (210).

12.   The computer readable storage medium as claimed in claim 11 further comprising a time stamp.

13.   A computer readable storage medium comprising a computer program for performing the following steps on an image:

dividing said image into a first plurality of cells having a first sequence (200);

generating a random seed (202);

generating a first plurality of pseudo random numbers based upon said random seed (204);

creating said image into a second plurality of cells based upon said first plurality of pseudo random numbers and said first plurality of cells (206);

generating a second plurality of pseudo random numbers, said second plurality of pseudo random numbers forming a second sequence (210);

comparing cells corresponding to said first sequence with cells corresponding to said second sequence, in forming a fingerprint (212).

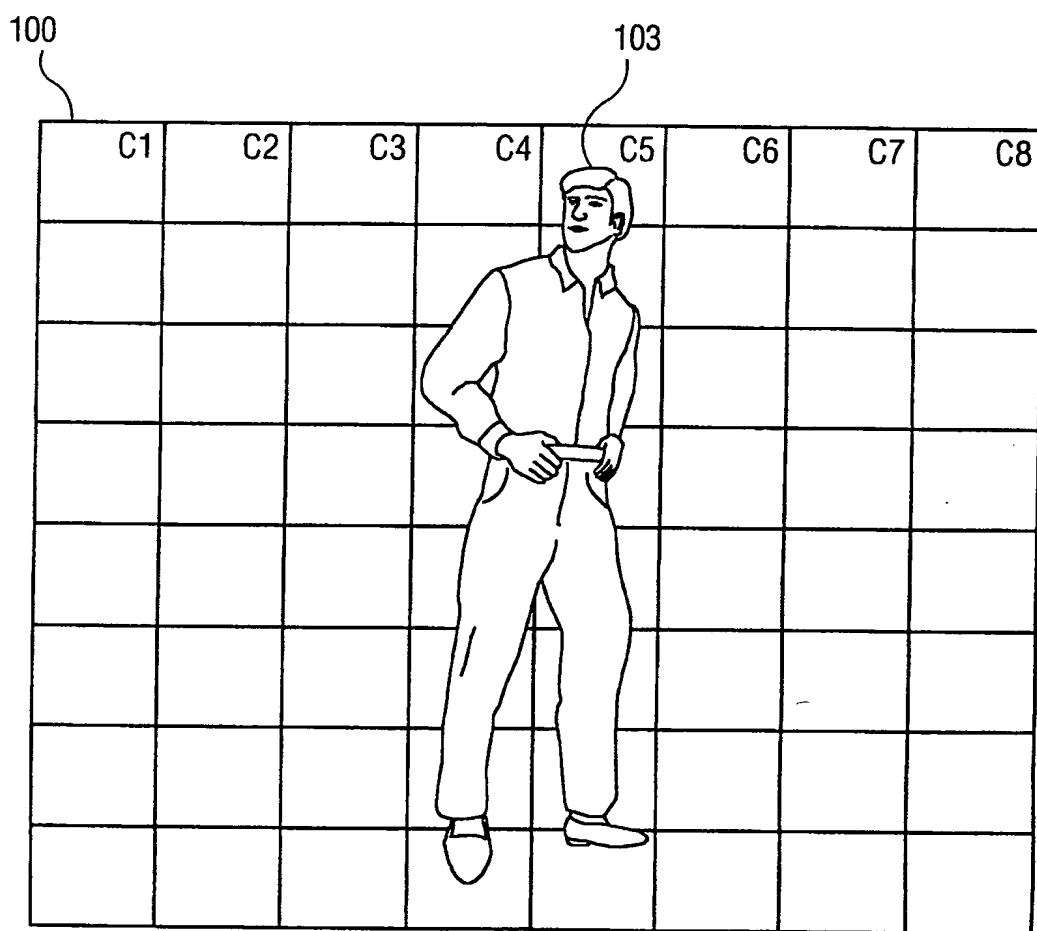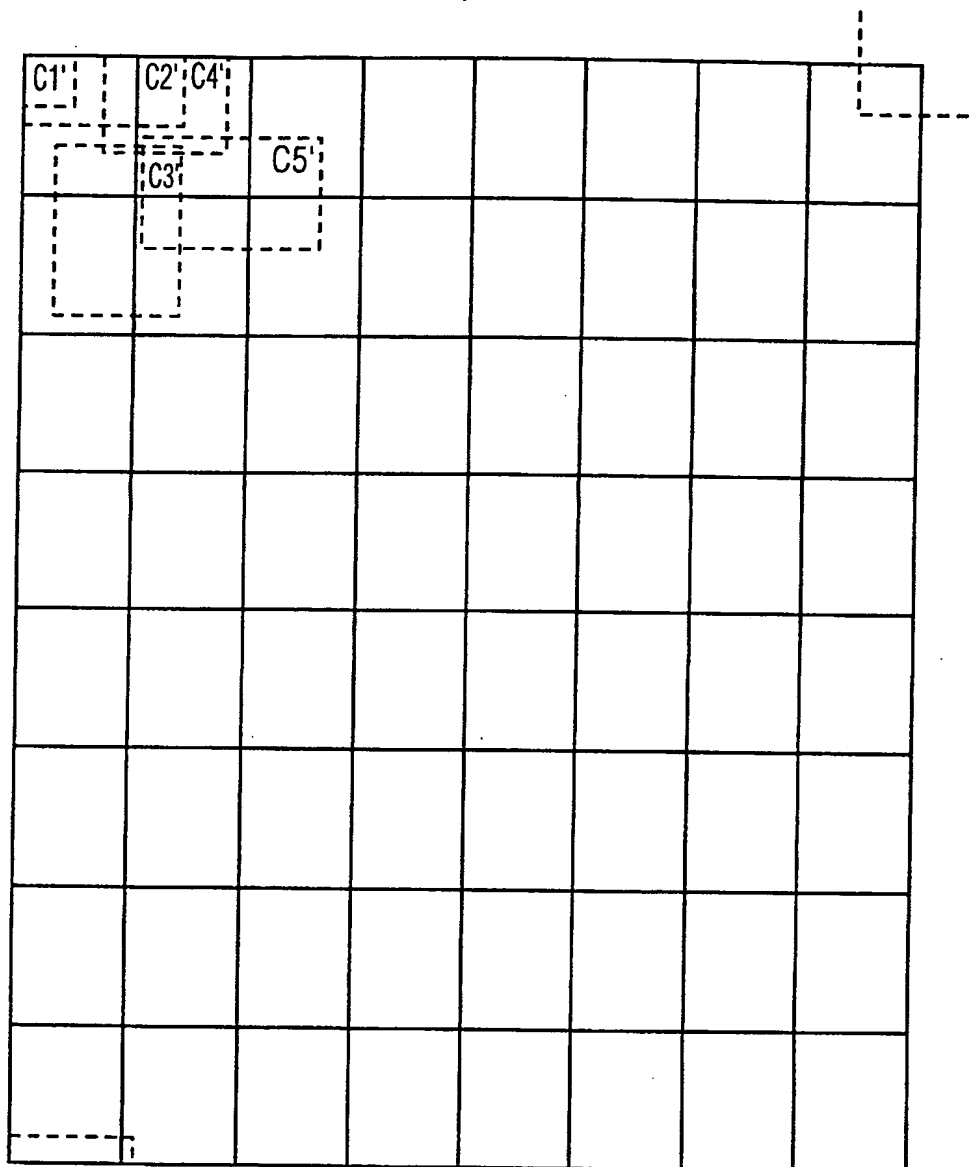FIG. 1

FIG. 2

FIG. 3
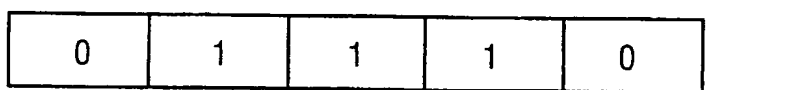
FIG. 4
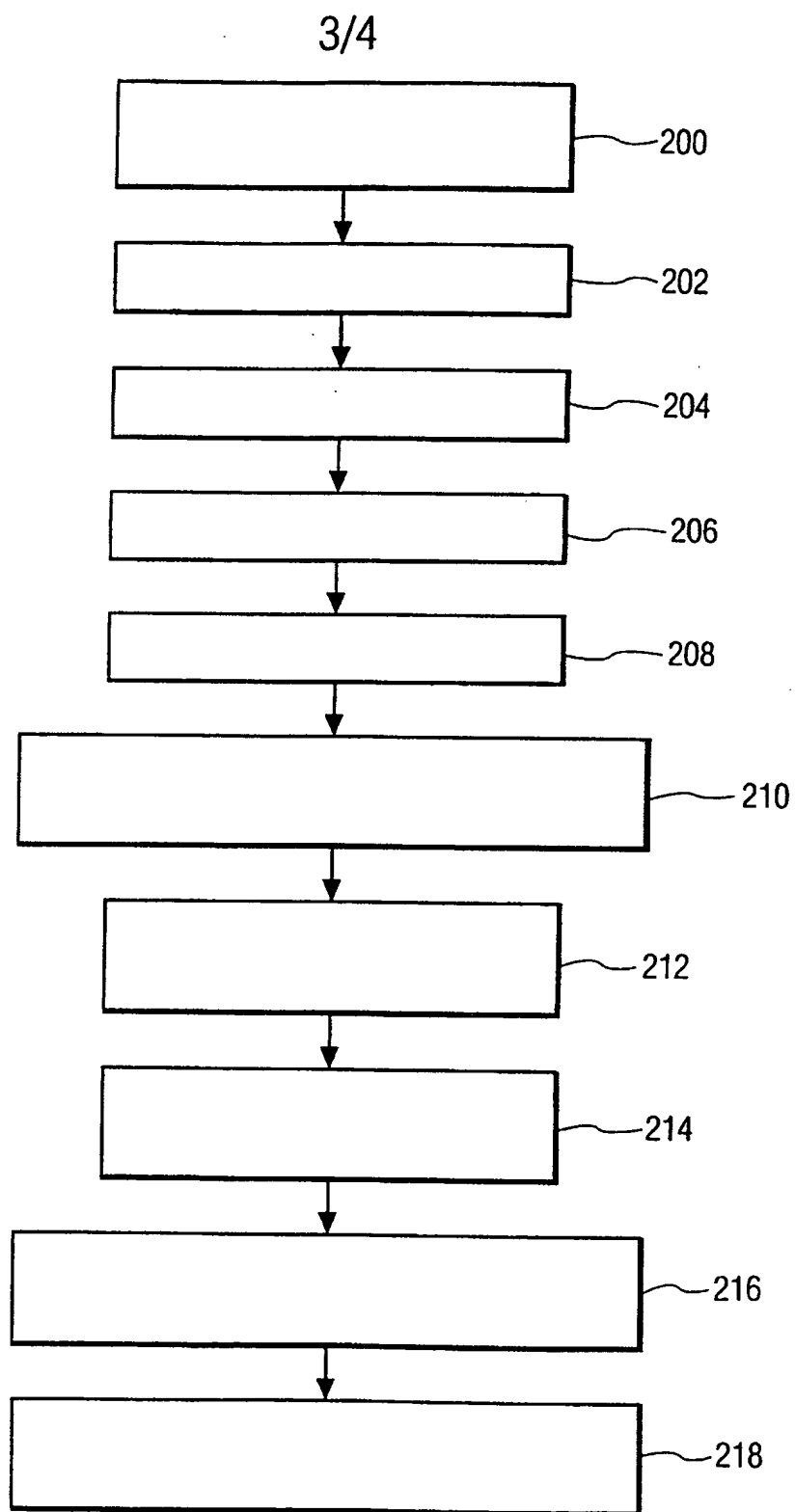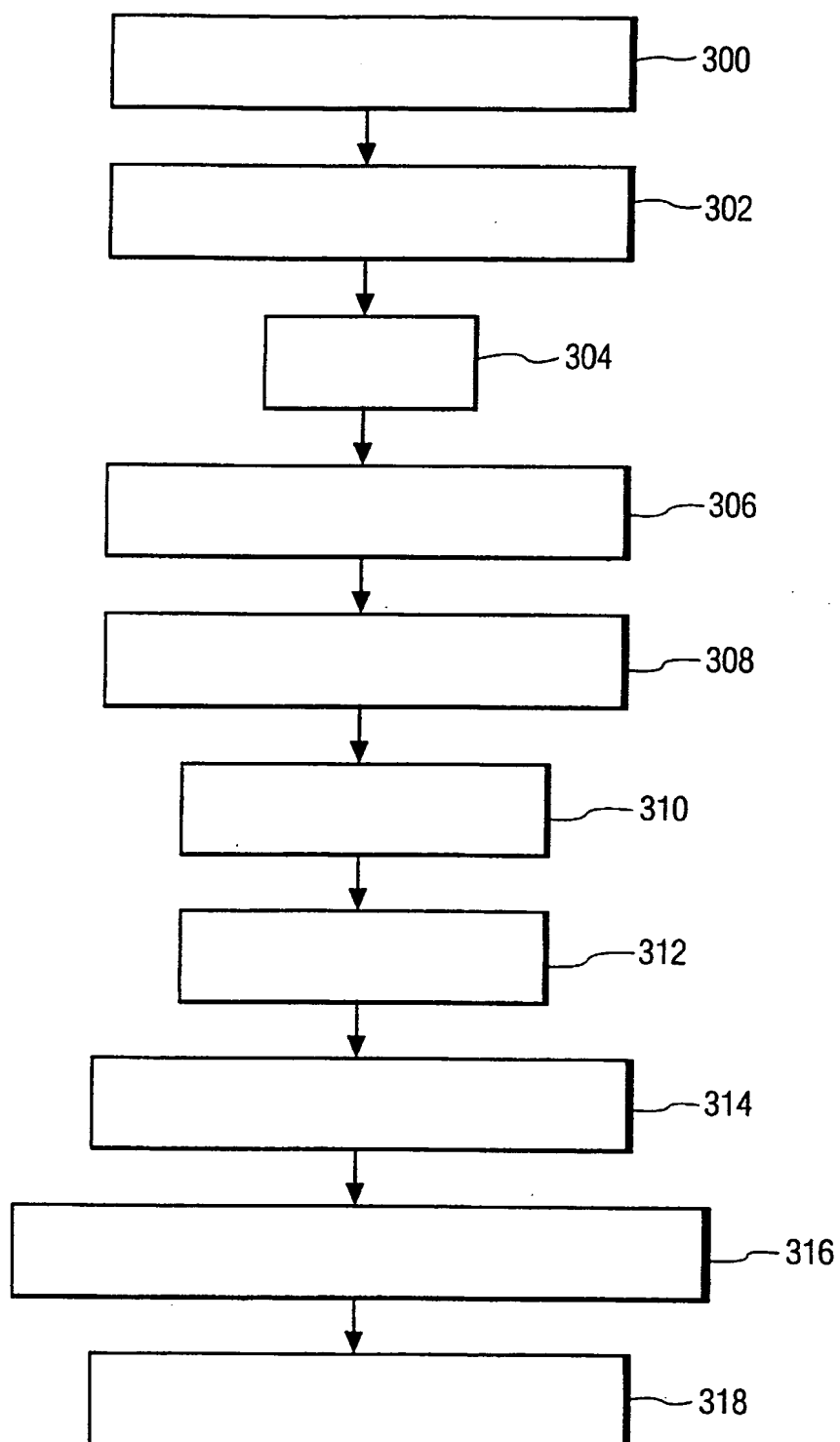
FIG. 5

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7   H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7   H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 95 20291 A (MOR LTD ;PAATELMA OTSO (GB); BORLAND ROD HUGH (GB)) 27 July 1995 (1995-07-27) abstract page 6, line 20 - line 31 page 7, line 5 - line 30 page 8, line 5 - line 18 claims 1-6 ---	1-13
A	US 5 189 700 A (BLANDFORD ROBERT R) 23 February 1993 (1993-02-23) abstract --- -/--	1-13

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 February 2000	10/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Stoffers, C

INTERNATIONAL SEARCH REPORT

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DAVERN P ET AL: "FRACTAL BASED IMAGE STEGANOGRAPHY" INFORMATION HIDING. INTERNATIONAL WORKSHOP PROCEEDINGS,XX,XX, 30 May 1996 (1996-05-30), pages 279-294, XP002048612 page 280 -page 281 ---	1-13
A	US 5 499 294 A (FRIEDMAN GARY L) 12 March 1996 (1996-03-12) abstract column 2, line 27 -column 3, line 56 figure 1 claims 1-6 ---	1-13
A	SZEPANSKI W: "A SIGNAL THEORETIC METHOD FOR CREATING FORGERY-PROOF DOCUMENTS FOR AUTOMATIC VERIFICATION" PROCEEDINGS OF THE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY: CRIME COUNTERMEASURES,US,NEW YORK, IEEE, vol. -, 1979, pages 101-109, XP002007950 abstract figure 2 -----	1-13

4

INTERNATIONAL SEARCH REPORT

.nformation on patent family members

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9520291	A	27-07-1995	AU	1422895 A	08-08-1995
US 5189700	A	23-02-1993	US	5347579 A	13-09-1994
			WO	9212485 A	23-07-1992
US 5499294	A	12-03-1996	NONE		